



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

08/999,766 07/23/97 MOSKOWITZ

S 2377/23

026118 TM02/0327
BROBECK, PHLEGER & HARRISON, LLP
ATTN: INTELLECTUAL PROPERTY DEPARTMENT
1333 H STREET, N.W. SUITE 800
WASHINGTON DC 20005

EXAMINER

MEISLAHN, D
ART UNIT PAPER NUMBER

2132
DATE MAILED:

03/27/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.
08/999,766

Applicant(s)
Moskowitz et al.

Examiner
Douglas Meislahn

Group Art Unit
2132



☒ Responsive to communication(s) filed on Jan 17, 2001

☒ This action is FINAL.

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) 25-63 is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) 25-63 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 17 January 2001 that amended claims 25 and 29.

Response to Arguments

2. Applicant's arguments with respect to claims 25-61 have been considered but are moot in view of the new ground(s) of rejection.
3. In view of applicant's discussion of claims 62 and 63, the 112 rejection is withdrawn. Applicant has provided a limitation of the term "imperceptible" that would be usable by a person of ordinary skill in the art.

Claim Rejections - 35 USC § 102

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 25, 27-29, 31-33, 35, 62, and 63 are rejected under 35 U.S.C. 102(a) as being anticipated by Bender et al. ("Techniques for data hiding").

In their introduction on page 164, Bender et al. distinguish between data hiding and encryption. They also state that hidden data should be "invisible" or "inaudible", which meets the limitations of claims 62 and 63. In the first paragraph of the next page, they say that watermarks are one type of data often inserted into files. In section 3.4, which studies spread spectrum environments, a pseudo-random key used to hide information is disclosed. The key, a carrier wave, and data are all combined. In section 1.2, Bender is mentioned as encrypting the embedded data. A reading of the section

Art Unit: 2767

cited as support for the amendment of 17 January 2001 seems to say that this feature is not inherent to a stega-cipher, but it is not quite entirely clear.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 26, 30, and 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Barton.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not say that the information includes a stream of digital samples. Barton's teaches embedding authentication information within a stream of digital data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate digital sample streams as in Barton with the key-encrypted watermarks of Bender et al.

Bender et al. teach encrypting digital watermarks into information with a key. They do not say that each sample has unique watermark information. In lines 20-33 of column 4, Barton teaches including sequence data with the authentication data. The authentication data is a reduced representation of digital data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Unique watermarks could also deter cryptanalysis attacks.

Pre-processing sample windows is inherent, as is determining which and how many windows will contain watermark information.

7. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not say that the information is then modified. Encryption modifies data. Official notice is taken that encrypting information in order to protect the data from unauthorized viewing is old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the watermarked data of Bender et al. by encrypting it.

8. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Morris.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that one bit is read out of every sample for the watermark. In lines 50-52 of the third column, Morris says that the human ear cannot detect the difference between a sound value of 64000 and 64001. This would be a one-bit change of the least significant bit. As taught by Morris, these small changes can be used to carry identification codes. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to discretely carry the watermark information of Bender et al. in the least significant bits as taught by Morris.

9. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Powell et al. (5930377).

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that samples are mapped to extract bits of information. As is explained in their abstract and diagrams, Powell et al. teach a method of embedding a digital watermark which requires use of a map of an image to determine the places to embed the watermark. This method is advantageous because, as explained in lines 42-43 of column 1, it is resistant to image modification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the mapping techniques of Powell to the encryption system of Bender et al. so as to make the data's watermark resistant to data modification.

10. Claims 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Braudaway et al.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not set out that the watermark is used in any specific manner.

By watermarking the data, Braudaway et al.'s method creates a first derivative encoded signal. It is inherent that attempts to decode the watermark without the proper key would further obfuscate the information. It was once theorized that encrypting information with two keys in order to strengthen security could in fact be mimicked by using one key that would possibly be easier to break. Although this theory has since been proven incorrect, the immediate solution was to strengthen security by encrypting with a first key and then decrypting with a non-corresponding second key. Providing information is inherent.

In the abstract, Braudaway et al. say that certain pixels brightness are altered as a result of the watermark. This change in brightness anticipates claim 38's spectral values. Also in the abstract, Braudaway et al. talk about using only certain non-transparent values of the watermark. These non-transparent values form a map to meet claim 39.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate any of the teachings of Braudaway into Bender et al.

11. Claims 40-43 and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Schneier.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets are used.

Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to

encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use mask sets to protect data.

12. Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier in view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that the data is spectrally spread before insertion of the digital watermarked. In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of watermark removal, and robustness, of their system of spectrally spreading data, inserting the watermark, and then putting the watermarked data through an inverse spectral spread. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to reap the benefits of Cox et al.'s method in Bender et al. and Schneier's system.

13. Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier as applied to claims 41, 48, and 29 above, and further in view of Barton.

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that a digital signature or hash of the start of message delimiter is validated. In his second figure, Barton shows a digital signature being used as an authentication tool. Digital signatures are made so that they are unique to the

article that they authenticate. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a digital signature, as taught by Barton, to verify the message sent by Bender et al. and Schneier.

14. Claims 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Barton as applied to claim 54 above.

Bender et al. teach encrypting digital watermarks into information with a key. They do not say that the data that is watermarked is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is old and well-known. The hash acts as a verification. Digital signatures with message appendix are a common term implementation of this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the

Art Unit: 2767

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

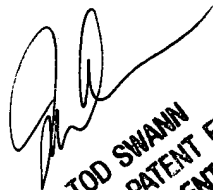
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached between 9 AM to 6 PM from Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-9051 for regular communications and (703) 308-9052 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
March 24, 2001



TOD SWANN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100